Amendment to the Claims:

This listing of claims will replace all versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for validating an electronic transmission, the method comprising the steps of:

generating a group key for encrypting and signing an electronic message transmitted on a network;

establishing a group key name corresponding to the group key for encrypting and signing the electronic message transmitted to a group of clients on the network;

transmitting a multicast data packet, the multicast data packet including the group key name, the electronic message and a signature to authenticate the electronic message and protect ~~and~~the group key name;

receiving the multicast data packet; [[and]]

validating the group key name in the received multicast data packet;

determining whether the group key name matches an entry in a group key name table at the receiver; and

discarding the received multicast data packet prior to attempting to decrypt the message body responsive to determining received group key name does not match an entry in the group key name table.

2. (Original) The method set forth in claim 1 further comprising the step of adding the group key name and the message authentication signature to a packet name extension prior to the step of transmitting.

3. (Original) The method set forth in claim 1 wherein the step of transmitting includes transmitting in accordance with an 802.11 protocol.

4. (Original) The method set forth in claim 1 further comprising the step of establishing an authenticated relationship.

5. (Original) The method set forth in claim 4 wherein the step of establishing an authenticated relationship employs a handshake protocol.

6. (Canceled)

7. (Original) The method set forth in claim 6 further comprising the steps of:

establishing a local group key name; and

storing the locally established group key name in the group key name table.

8. (Original) The method set forth in claim 1 further comprising the step of encrypting the multicast message prior to transmission.

9. (Original) The method set forth in claim 1 further comprising the step of decrypting the received multicast message if the received group key name matches an entry in the group key name table.

10. (Canceled)

11. (Currently Amendedl) A system for targeting multicast transmission, the system comprising:

means for generating a group key for signing a multicast message transmitted via a network;

means for generating a group key name for naming the group key;

means for combining the group key name to the multicast message to form a multicast packet;

means for transmitting the multicast packet to a receiver via the network;

means for receiving the multicast packet;

means for validating the received group key name contained within the received multicast packet; ~~and~~

means for determining whether the ~~intended group recipients based upon the~~ validated group key name matches an entry in a group key name table at the receiver; and

means for discarding the received multicast data packet prior to attempting to decrypt the message body responsive to determining received group key name does not match an entry in the group key name table.

12. (Canceled)

13. (Original) The system set forth in claim 11 wherein the means for transmitting the management frame packet is an IEEE 802.11 protocol.

14. (Original) The system set forth in claim 11 wherein the means for generating a group key is in accordance with an IEEE 802.1 pre-standard.

15. (Original) The system set forth in claim 11 wherein the group key name is a unique identifying element.

16. (Original) An article of manufacture embodied in a computer-readable medium for use in a processing system for transmitting electronic messages to and/or from a network, the article comprising:

a group key generation logic for causing a processing system to generate a group key for encrypting and signing an electronic message transmitted on a network;

a group key name generation logic for causing a processing system to generate a group key name for encrypting and signing the electronic message transmitted on the network;

a data transmitting logic for causing a processing system to transmit the electronic message to a group of clients on the network; ~~and~~

a message receiving logic for causing a processing system to verify whether a receiving client is an intended recipient of the electronic message; and

a message discarding logic for causing a processing system to discard the received multicast data packet prior to attempting to decrypt the message body responsive to determining received group key name does not match an entry in the group key name table at the receiving client.

17. (Original) The article as set forth in claim 16 wherein the data transmitting logic includes an IEEE 802.11 protocol.

18. (Original) The article as set forth in claim 16 wherein the message receiving logic further includes means for causing a processing system to compare a received group key name with a local key name table.